UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
SOUTHERN DIVISION

CHRIS CERVANTES
34632 CHILTON AVE
PINE, CO 80470-9526
On behalf of Himself and All Others Similarly Situated,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC.
10400 FERNWOOD RD
BETHESDA, MD 20817
MONTGOMERY COUNTY
SERVE ON: THE CORPORATION TRUST INCORPORATED
2405 YORK ROAD, SUITE 201
LUTHERVILLE TIMONIUM, MD 21093-2264,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Chris Cervantes ("Cervantes" or "Plaintiff") individually and on behalf of the proposed Classes initially defined below, brings this Class Action Complaint ("Complaint") against Marriot International, Inc. (hereafter "Marriott" or "Defendant"). Plaintiff brings this action based upon his counsel's investigation and personal knowledge of the facts pertaining to himself, and on belief as to all other matters where noted, by and through undersigned counsel.

NATURE OF THE CASE

1. This class action seeks to redress Marriott's unlawful and negligent disclosure of millions of consumers' confidential personal information, including their names, addresses,

passport details, phone numbers, email addresses, dates of birth, gender, travel details, credit and debit card numbers, and other payment information (hereafter, "Personal Information").

2. In a November 30, 2018 statement, Marriott revealed that the Personal Information of approximately 500 million guests was exposed in a breach that allowed unauthorized access to its Starwood Hotels reservation database (the "Data Breach").[1]

3. Specifically, according to Marriott's investigation to date, between at least 2014 and September 2018, hackers had unabated access to the Personal Information of approximately 500 million guests who made a reservation at Marriott's Starwood properties.

4. This breach is considered one of the longest-running and largest data breaches in history. And it could have been prevented. Numerous other hotel chains, including, but not limited to Hilton, Mandarin Oriental, and the Trump Collection have been hit with similar data breaches. While many retailers, banks, and credit card companies responded to recent breaches by adopting technology that helps make transactions and databases more secure, Marriott did not.

5. Despite the fact that the threat of a data breach has been a well-known risk in the hospitality industry, Marriott failed to take reasonable steps to adequately protect the ultra-sensitive, highly sought after personal data and payment information of hundreds of millions of individuals.

6. Defendant's data security deficiencies were so significant that, even after hackers entered its systems, their activities went undetected for at least four years.

[1] *See* http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last visited Dec. 5, 2018).

7. Plaintiff and the members of proposed Classes are now left to deal with the direct consequences of Defendant's failures. Plaintiff seeks to recover compensation for the time and costs that he and others similarly situated have been, or will be, forced to bear as a direct result of Defendant's Data Breach and to obtain appropriate equitable and injunctive relief to mitigate future harm that is certain to occur in light of Marriott's extremely lax approach to security and the unprecedented scope of this breach.

PARTIES

8. Plaintiff Chris Cervantes is a citizen and resident of the State of Colorado. Plaintiff, a member of Marriott's Starwood program, has stayed at Marriott properties for approximately six years. Plaintiff provided his personal and financial information to Defendant on the basis that Defendant would maintain his personal and financial information safe and secure; would employ reasonable and adequate security measures to ensure that hackers would not compromise his information; and notify him promptly in the event of a breach. On December 3, 2018 and on December 6, 2018, Defendant provided Plaintiff email notices that his information was compromised by the Data Breach. (*See* attached hereto as Exhibit A). Due to the Data Breach, Plaintiff is taking measures that he otherwise would not have to take to ensure that his identify is not stolen and that his accounts are not compromised.

9. Defendant Marriott International, Inc. is a Delaware corporation with its principal place of business in Bethesda, Maryland. Marriott is principally a hotel and restaurant business. Starwood became a wholly-owned subsidiary of Marriott in 2016.

JURISDICTION AND VENUE

10. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest

and costs; the number of members of each of the proposed Classes exceed 100; and many members of the proposed Classes are citizens of states different from Defendant.

11. This Court has personal jurisdiction over Defendant as it is headquartered in this State and in this District and/or has sufficient minimum contacts with this State.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and because Defendant is headquartered in this District.

FACTUAL ALLEGATIONS

A. Marriott Collects and Stores Massive Amounts of Private Information from Its Guests

13. Marriott is the largest hotel chain in the world, with more than 6,500 properties located in 127 countries and territories globally. Marriott owns and operates a variety of hotel, lodging, and hospitality brands, including hotels under the Starwood brands.[2] Hundreds of millions of customers have made reservations and have stayed at Marriott properties around the world.

14. When booking reservations at Marriott properties, including the Starwood brand properties, customers provide Marriott with sensitive personal information, including names, addresses, passport numbers, email addresses, dates of birth, gender, and payment information.

15. On its website, Marriott states that the type of personal data it collects includes:

- Name;
- Gender;
- Postal address;
- Telephone number;

[2] The Starwood properties include: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels. Starwood branded timeshare properties are also included.

- Email address;
- Credit and debit card number or other payment data;
- Financial information in limited circumstances;
- Language preference;
- Date and place of birth;
- Nationality, passport, visa or other government-issued identification data;
- Important dates, such as birthdays, anniversaries, and special occasions;
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations);
- Employer details;
- Travel itinerary, tour group, or activity data;
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests;
- Geolocation information; and
- Social media account ID, profile photo, and other data publicly available, or data made available by linking your social media and loyalty accounts.[3]

16. Further, Marriott states that it may also collect:

- Data about family members and companions, such as names and ages of children;
- Biometric data, such as digital images;
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel; and
- Guest preferences and personalized data ("Personal Preferences"), such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit.[4]

17. Individuals who entrust Marriott with their sensitive data do so with the understanding that Marriott will safeguard their Personal Information.

B. <u>The Marriott Data Breach</u>

18. On November 30, 2018, Marriott announced that hackers accessed its Starwood reservation system and stole the Personal Information of approximately 500 million guests who made reservations at Starwood properties.

[3] Marriott, https://www.marriott.com/about/privacy.mi (last visited Dec. 5, 2018).

[4] *Id.*

19. Marriott claims it discovered the security breach on September 8, 2018, "from an internal security tool regarding an attempt to access the Starwood guest reservation database," and "quickly engaged leading security experts to help determine what occurred."[5]

20. Marriott subsequently learned through an investigation that there had been unauthorized access to the Starwood network since 2014.[6] In other words, the Data Breach affects customers who made reservations for Starwood hotel brand properties from 2014 through September of 2018. The amount of time it normally takes to discover a breach, also known as "dwell time" in the security industry, is 101 days. Thus, the dwell time in this case is astoundingly large.

21. According to Marriott, for approximately 327 million guests, the information stolen includes names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest ("SPG") account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences.[7] For some guests, the information also includes credit card numbers and expiration dates.[8] While the payment card numbers were encrypted, and there are two components needed to decrypt the payment card numbers, Marriott has not been able to rule out the possibility that both were taken.[9]

22. The hospitality industry has become a target of cyber-attacks. Many other hospitality chains have been subject to major data and security breaches. Since the hospitality

---

[5] Kroll, *Starwood Guest Reservation Database Security Incident*, (updated Dec. 8, 2018), https://answers.kroll.com/.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

industry has become a target for attackers, Marriott was clearly aware of this threat. Indeed, Marriott was subject to a smaller data breach in 2015 where attackers installed malware on its point of sale systems in some of its hotels.

23. Yet Marriott failed to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and members of the Classes' sensitive Personal Information. Moreover, Marriott failed to protect against reasonably foreseeable threats to the security of Plaintiff's and members of the Classes' sensitive Personal Information and failed to discover the attack announced in November 2018 sooner, although a thorough investigation of its 2015 data breach should have revealed this current data breach according to security experts.

24. Gus Hosein, Executive Director of Privacy International, a group that supports strong data protection laws, stated, "[t]hey can say all they want that they take security seriously, but they don't if you can be hacked over a four-year period without noticing."[10]

C. Marriott's Post-Breach Response Is Deficient

25. Arne Sorenson, Marriott's President and Chief Executive, said in a statement, "[w]e deeply regret this incident," and "[w]e fell short of what our guests deserve and what we expect of ourselves."[11] As a consolation, Marriott is offering its guests one year of "WebWatcher" free of charge. WebWatcher is a service that monitors internet sites where personal information is shared, and alerts consumers if evidence of the consumer's personal information is found.

[10] Nicole Perlroth, et al., *Marriott Hacking Exposes Data of Up to 500 Million Guests*, The New York Times (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

[11] *Id.*

26. However, one year of WebWatcher is woefully inadequate. With only one year of WebWatcher and no form of insurance or other protection, Plaintiff and members of the Classes remain unprotected from the real and long-term threats against their Personal Information. One year of WebWatcher only means that cybercriminals must simply wait one year before they can share, use, or purchase the stolen data on the internet.

27. Additionally, cybercriminals can commit identity theft and all of the collateral damage that comes along with it without sharing the Personal Information on Internet sites.

D. Plaintiff and Members of the Classes Suffered Damages

28. Plaintiff's and members of the Classes' sensitive Personal Information was left inadequately protected by Marriott and thus, Plaintiff and members of the Classes will have to take significant steps to protect themselves for several years to come, including buying credit monitoring and identity protection, possibly replacing passports and changing passwords, among other things. In fact, Senate Minority Leader Charles E. Schumer has suggested that Marriott should cover the cost of affected customers' passport replacement.

29. The Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiff's and members of the Classes' sensitive Personal Information from unauthorized access, capture, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law.

30. Defendant's negligence, wrongful actions, and inaction have caused Plaintiff and members of the Classes to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including, but not limited to:

a. theft of their personal and financial information;

b. the imminent and impending injury flowing from potential fraud and identify theft posed by their personal information being placed in the hands of criminals;

c. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

d. ascertainable losses in the form of deprivation of the value of their personal and sensitive data, for which there is a well-established national and international market;

e. injuries caused by the untimely and inadequate notification of the data breach; and

f. the deprivation of rights they possess under various state laws.

31. Additionally, Plaintiff and members of the Classes were overcharged when they paid for and used Defendant's services and properties. A portion of the price paid for such products and services to Marriott was for the costs of reasonable and adequate safeguards and security measures that would protect customers' sensitive Personal Information, which Marriott did not implement and, as a result, Plaintiff and members of the Classes did not receive what they paid for.

CLASS ACTION ALLEGATIONS

32. Plaintiff brings this action on behalf of himself and two classes: a Nationwide Class and a Colorado Subclass (together "Classes").

33. The Nationwide Class is initially defined as follows:

> **"All persons in the United States whose personal and/or financial information was accessed, compromised, or stolen in the Data Breach announced by Marriott in November 2018."**

Excluded from the Nationwide Class are Defendant, its corporate parents, subsidiaries, affiliates, officers, directors, employees, agents, and any entity in which Defendant has a controlling interest, as well as the Court and its personnel presiding over this action.

34. The Colorado Subclass is initially defined as follows:

> **"All persons in the State of Colorado whose personal and/or financial information was accessed, compromised, or stolen in the Data Breach announced by Marriott in November 2018."**

Excluded from the Colorado Subclass are Defendant, its corporate parents, subsidiaries, affiliates, officers, directors, employees, agents, and any entity in which Defendant has a controlling interest, as well as the Court and its personnel presiding over this action.

35. Plaintiff reserves the right to amend the class definition(s) or to define classes and subclasses as required, based on the investigation and research of his counsel.

36. This action has been properly brought and may properly be maintained as a class action under Rule 23(a)(1-4), Rule 23(b)(1), (2) or (3), and/or Rule 23(c)(4) of the Federal Rules of Civil Procedure and case law thereunder.

Numerosity of the Classes

(Fed. R. Civ. P. 23(a)(1))

37. Members of each Class are so numerous that their individual joinder is impractical. The Classes comprise, at the least, millions of people. According to Marriott, approximately 500 million customers had their personal and/or financial information compromised during the Data Breach. The precise number of the members of each Class, and their addresses are unknown to Plaintiff at this time, but can be ascertained from Defendant's

records. Members of the Classes may be notified of the pendency of this action by mail or email, supplemented (if deemed necessary or appropriate by the Court) by published notice.

Predominance of Common Questions of Fact and Law

(Fed. R. Civ. P. 23(a)(2); 23(b)(3))

38. Common questions of law and fact exist as to all members of the Classes. These questions predominate over the questions affecting only individual members of the Classes. The common legal and factual questions include, without limitation:

(a) Whether Defendant represented that its guests' Personal Information in its custody was secure when in fact it was not;

(b) Whether Defendant failed to disclose that Personal Information entrusted to it was at risk of being improperly accessed, compromised, and/or stolen owing to Defendant's inadequate security procedures or reckless policies;

(c) Whether Defendant owed a duty to Plaintiff and members of the Classes to adequately protect their Personal Information;

(d) Whether Defendant breached their duties to protect the Personal Information of Plaintiff and members of the Classes;

(e) Whether Defendant knew or should have known that their data security systems and processes were vulnerable to attack;

(f) Whether Plaintiff and members of the Classes suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of identity theft and loss of value of their Personal Information;

(g) Whether Defendant negligently failed to warn Plaintiff and members of

the Classes that their Personal Information entrusted to it was not properly protected and that it did not maintain the security procedures and measures reasonably necessary to protect such data from compromise;

(h) Whether Defendant has an implied contractual obligation to use reasonable security measures;

(i) Whether Defendant has complied with any implied contractual obligation to use reasonable security measures; and

(j) Whether Plaintiff and members of the Classes are entitled to equitable relief, including injunctive relief.

Typicality of Claims

(Fed. R. Civ. P. 23(a)(3))

39. Plaintiff's claims are typical of the claims of the Classes because Plaintiff, like all proposed members of the Classes, had his Personal Information in Defendant's custody compromised in the Data Breach.

Adequacy of Representation

(Fed. R. Civ. P. 23(a)(4))

40. Plaintiff is an adequate representative of the Classes, because his interests do not conflict with the interests of the members of the Classes and he has retained counsel competent and experienced in complex class action and consumer litigation.

41. Plaintiff and his counsel will fairly and adequately protect the interests of the members of the Classes.

Superiority of a Class Action

(Fed. R. Civ. P. 23(b)(3))

42. A class action is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and members of the Classes. The damages suffered by each individual member of the Classes, while significant, are small given the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. Further, it would be virtually impossible for the members of the Classes individually to redress effectively the wrongs done to them. And, even if members of the Classes themselves could afford such individual litigation, the court system could not, given the many thousands – or even millions -- of cases that would need to be filed. Individualized litigation would also present a potential for inconsistent or contradictory judgments. Individualized litigation would increase the delay and expense to all parties and the court system, given the complex legal and factual issues involved. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief

(Fed. R. Civ. P. 23(b)(1) And (2))

43. In the alternative, this action may properly be maintained as a class action, because:

(a) the prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudication with respect to individual members of the Classes, which would establish incompatible standards of conduct for Defendant; or

(b) the prosecution of separate actions by individual members of the Classes would create a risk of adjudications with respect to individual members of the Classes which

would, as a practical matter, be dispositive of the interests of other members of the Classes not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

(c) Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby making appropriate final injunctive or corresponding declaratory relief with respect to each Class as a whole.

Issue Certification

(Fed. R. Civ. P. 23(c)(4))

44. In the alternative, common questions of fact and law, including those set forth in paragraph 38, above are appropriate for issue certification.

FIRST CAUSE OF ACTION

(For Negligence and Negligent Failure to Warn)

(On Behalf of Plaintiff and the Classes)

45. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of the Classes.

46. Defendant's actions constitute negligence and/or negligent failure to warn.

47. Defendant owed a duty of care to Plaintiff and the members of the Classes to exercise reasonable care in obtaining and protecting their Personal Information, and keeping it from being improperly accessed, compromised, and/or stolen. Defendant breached that duty by failing to take appropriate and adequate security measures to protect and secure Plaintiff's and members of the Classes' Personal Information.

48. When Plaintiff and members of the Classes provided their Personal Information to Defendant, they had the reasonable belief that Defendant would take appropriate and adequate

measures to secure and protect their information, and would warn them of dangers and inform them of any breaches or other security concerns that might call for action by them. In violation of that duty, Defendant failed to warn them of dangers inherent in its databases and/or its system and failed to prevent third parties, including hackers, from improperly obtaining Plaintiff's and members of the Classes' Personal Information.

49. Among other things, Defendant failed to warn Plaintiff and members of the Classes that their Personal Information entrusted to Defendant was not properly protected and that Defendant did not maintain the security procedures and measures reasonably necessary to protect such data from unauthorized access by hackers.

50. Among other things, Defendant failed to implement and maintain the security procedures, measures, and protocols reasonably necessary to protect Plaintiff's and members of the Classes' personal and financial information from unauthorized access by hackers.

51. Among other things, Defendant failed to notify Plaintiff and members of the Classes in a timely manner that their Personal Information had been taken by third parties and of the danger to them caused by the Data Breach.

52. As a direct and proximate result of the practices, acts, and omissions alleged herein, Plaintiff and members of the Classes have suffered injury and damages.

53. At all relevant times, Plaintiff and members of the Classes acted lawfully and with due care and did not contribute to the injuries suffered.

54. Plaintiff and members of the Classes are entitled to damages and other relief, as prayed for hereunder.

SECOND CAUSE OF ACTION

(Negligence Per Se)

(On Behalf of Plaintiff and the Classes)

55. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of the Classes.

56. Defendant violated Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45 by failing to provide reasonable security to prevent unauthorized access to Plaintiff's and members of the Classes' Personal Information in databases stored by Defendant.

57. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair practices of failing to use reasonable security measures to protect the personal and financial information of consumers. The FTC publications concerning data security and data security orders further form the basis of Defendant's violation of Section 5 of the FTCA.

58. Defendant's conduct caused the type of harm that Section 5 of the FTCA was intended to prevent. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Classes.

59. Plaintiff and members of the Classes are within the class of persons that Section 5 of the FTCA was intended to protect. Defendant knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify Plaintiff and members of the Classes would cause damages to Plaintiff and members of the Classes.

60. Defendant's violation of Section 5 of the FTCA constitutes negligence per se.

61. But for Defendant's violation of Section 5 of the FTCA, Plaintiff's and members of the Classes' Personal Information would not have been accessed by unauthorized individuals.

62. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Classes have suffered, and will continue to suffer, injury and damages, which includes but is not limited to exposure to heightened, imminent risk of fraud, identify theft, and financial harm. Plaintiff and members of the Classes must monitor their financial accounts and credit histories more closely and frequently to guard against identify theft. Members of the Classes also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect fraud and identity theft. The unauthorized acquisition of Plaintiff's and members of the Classes' Personal Information also diminished the value of their Personal Information.

63. The damages to Plaintiff and the members of the Classes were a proximate and reasonably foreseeable result of Defendant's breach of Section 5 of the FTCA. Therefore, Plaintiff and members of the Classes are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION

(Breach of Implied Contract)

(On Behalf of Plaintiff and the Classes)

64. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of the Classes.

65. Plaintiff and members of the Classes entered into implied contracts with Defendant when Defendant solicited and invited Plaintiff and members of the Classes to stay at its Starwood properties by requiring Plaintiff and members of the Classes to provide their Personal Information, including their Starwood loyalty program account information, to its Starwood guest reservation database.

66. When Plaintiff and members of the Classes provided their Personal Information to Defendant, Defendant implicitly agreed that it would protect and safeguard their Personal Information by using reasonable security measures, and would timely and accurately notify Plaintiff and members of the Classes in the event of a data breach.

67. Plaintiff and members of the Classes would not have provided their Personal Information in connection with their reservations, including joining Starwood's loyalty program, to Defendant had they known that Defendant would not protect and safeguard their Personal Information.

68. Plaintiff and members of the Classes fully performed their obligations under the implied contracts with Defendant.

69. Defendant breached the implied contracts with Plaintiff and members of the Classes by failing to protect and safeguard the Personal Information of Plaintiff and members of the Classes, and by failing to provide timely and accurate notice to Plaintiff and members of the Classes that their Personal Information was compromised in the Data Breach.

70. As a direct and proximate result of Defendant's breaches of the implied contracts with Plaintiff and members of the Classes, Plaintiff and members of the Classes suffered, and continue to suffer, injuries and damages.

FOURTH CAUSE OF ACTION

(Violation of the Maryland Consumer Protection Act, Md. Comm. Code §§ 13-101, *et seq*.)

(On Behalf of Plaintiff and the Nationwide Class)

71. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of the Nationwide Class.

72. Defendant's business practices as complained of herein violate the Maryland Consumer Protection Act, Md. Comm. Code §§ 13-101, *et seq*. ("MCPA").

73. Plaintiff and members of the Nationwide Class are "consumers" as defined by Md. Comm. Code § 13-101(c).

74. Defendant is a "person" as defined by Md. Comm. Code § 13-101(h). Defendant is also a "merchant" as defined by Md. Comm. Code § 13-101(g).

75. Defendant advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

76. Defendant engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

(a) False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

(b) Failing to state a material fact where the failure deceives or tends to deceive;

(c) Advertising or offering consumer goods or consumer services without intent to sell, lease, or rent them as advertised or offered;

(d) Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of any consumer goods, or consumer services or the subsequent performance with respect to an agreement, sale lease or rental.

77. Defendant also engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-303 in connection with offering for sale or selling consumer goods or consumer services or with respect to the extension of consumer credit, including:

(a) Failing to implement and maintain reasonable security measures to protect and safeguard Plaintiff's and the Nationwide Class members' Personal Information, which was a direct and proximate cause of the Data Breach;

(b) Misrepresenting or omitting material facts to Plaintiff and the Nationwide Class members regarding the adequacy of its data security measures in protecting and safeguarding Plaintiff's and the Nationwide Class members' Personal Information;

(c) Failing to identify foreseeable data security risks, remediate identified data security risks, and adequately improve data security measures following previous cyber security incidents, which was a direct and proximate cause of the Data Breach;

(d) Failing to inform and disclose the Data Breach to Plaintiff and the Nationwide Class members in a timely and accurate manner;

(e) Failing to comply with relevant state and federal laws pertaining to the security of Plaintiff's and the Nationwide Class members' Personal Information, which was a direct and proximate cause of the Data Breach;

78. Defendant's representations and omissions were material because they were likely to deceive and did deceive Plaintiff and the Nationwide Class members regarding the adequacy of Defendant's data security measures and ability to protect and safeguard their Personal Information. Defendant's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

79. Defendant intentionally and knowingly misrepresented such material facts with intent to mislead Plaintiff and the Nationwide Class members. Plaintiff and the Nationwide Class members were induced to rely on Defendant's misrepresentations and omissions.

80. Defendant acted intentionally, knowingly, and maliciously to violate the Maryland Consumer Protection Act, and recklessly disregarded Plaintiff's and the Nationwide Class members' rights in having their Personal Information protected and safeguarded.

81. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and the Nationwide Class members have suffered, and will continue to suffer, injury and damages, which includes but is not limited to exposure to heightened, imminent risk of fraud, identify theft, and financial harm. Plaintiff and the Nationwide Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identify theft. The Nationwide Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect fraud and identity theft. The unauthorized acquisition of Plaintiff's and the Nationwide Class members' Personal Information also diminished the value of their Personal Information.

82. Plaintiff and the Nationwide Class members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

FIFTH CAUSE OF ACTION

(Violation of the Maryland Personal Information Protection Act,

Md. Comm. Code §§ 14-3501, *et seq*.)

(On Behalf of Plaintiff and the Nationwide Class)

83. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of the Nationwide Class.

84. Defendant's business practices as complained of herein violate the Maryland Personal Information Protection Act, Md. Comm. Code §§ 14-3501, *et seq*. ("MPIPA").

85. Plaintiff's and the Nationwide Class members' Personal Information, as described herein, includes "personal information" as defined under Md. Comm. Code § 14-3501(d), such as a social security number, a passport number, a driver's license number, a credit or debit card number, and/or user name or e–mail address in combination with a password or security question and answer that permits access to an individual's e–mail account.

86. Plaintiff and the Nationwide Class members are "individuals" and "customers" as defined by Md. Comm. Code §§ 14-3502(a) and 14-3503.

87. Defendant is a business that owns or licenses computerized data that includes personal and financial information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

88. The Defendant's Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(1).

89. Under Md. Comm. Code § 14-3503(a), "[t]o protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."

90. Under Md. Comm. Code § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a

reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach."

91. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach of the security of a system."

92. When Defendant discovered the Data Breach and it had notice of the Data Breach, Defendant was obligated to disclose the Data Breach in a timely and adequate manner as required by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

93. By failing to disclose the Data Breach in a timely and adequate manner, Defendant violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

94. As a direct and proximate result of Defendant's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and the Nationwide Class members suffered damages, as alleged above.

95. Under Md. Comm. Code § 14-3508, Defendant's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the MCPA, and subject to the enforcement and penalty provisions contained in the MCPA.

96. Pursuant to Md. Comm. Code § 14-3508, Plaintiff and the Nationwide Class members seek relief, including damages and attorneys' fees.

SIXTH CAUSE OF ACTION

(Violation of the Colorado Consumer Protection Act, Colo. Rev. Stat. §§ 6-1-101, *et seq*.)

(On Behalf of Plaintiff and the Colorado Subclass)

97. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of the Colorado Subclass.

98. Plaintiff and Colorado Class members were and/or consumers of Defendant's services and injured due to Defendant's deceptive trade practices.

99. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the course of Defendant's business, vocation, or occupation in violation of C.R.S. § 6-1-105, including but not limited to the following:

(a) Defendant knowingly misrepresented and fraudulently advertised material facts pertaining to its reservation and booking process for staying at a Marriott property to Plaintiff and the Colorado Class members by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Colorado Class members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Colo. Rev. Stat. § 6-1-105(1)(e), (g), (i), and (u);

(b) Defendant knowingly misrepresented material facts pertaining to its reservation and booking process for staying at a Marriott property to Plaintiff and the Colorado Class members by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Colorado Class members' Personal Information, in violation of Colo. Rev. Stat. § 6-1-105(1)(e), (g), (i), and (u);

(c) Defendant knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Colorado Class

members' Personal Information (intending to induce others to enter into a transaction), in violation of Colo. Rev. Stat. § 6-1-105(1)(e), (g), (i), and (u);

(d) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of C.R.S. § 6-1-105(3), by failing to maintain the privacy and security of Plaintiff's and Colorado Class members' Personal Information, and in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act, 15 U.S.C. § 45, negligence, and breach of implied contract;

(e) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of C.R.S. § 6-1-105(3), by failing to disclose the Data Breach to Plaintiff and Colorado Class members in a timely and accurate manner, contrary to the duties imposed by Colo. Rev. Stat. Ann. § 6-1-716(2);

(f) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of C.R.S. § 6-1-105(3) by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Colorado Class members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

100. Defendant engaged in the above or deceptive acts or practices in the course of its business.

101. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Colorado Class members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their Personal Information.

102. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

103. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Colorado Class members' Personal Information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff and members of the Colorado Class.

104. Plaintiff and Colorado Class members seek relief under Colo. Rev. Stat. §§ 6-1-101, *et. seq*., including, not limited to, compensatory damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the proposed Classes pray for relief and judgment against Defendant, as follows:

A. Certifying the Classes pursuant to Rule 23 of the Federal Rules of Civil Procedure, certifying Plaintiff as representative of the Classes and designating his counsel as counsel for the Classes;

B. Awarding Plaintiff and the Classes compensatory damages, in an amount exceeding $5,000,000, to be quantified by competent evidence and expert analysis;

C. Awarding Plaintiff and the Classes statutory damages;

D. Awarding Plaintiff and the Classes punitive damages;

E. For declaratory and equitable relief, including restitution and disgorgement;

F. For injunctive relief, including without limitation requiring Defendant to take steps to repair the injury caused by its negligence and wrongful conduct;

G. Awarding Plaintiff and the Classes the costs of prosecuting this action, including expert witness fees;

H. Awarding Plaintiff and the Classes reasonable attorneys' fees;

I. Awarding pre-judgment and post-judgment interest; and

J. Granting other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury of all claims so triable.

Dated: December 13, 2018

LEVI & KORSINSKY, LLP

By: */s/Donald J. Enright*

Donald J. Enright, Esq. (Bar No. 13551)
Email: denright@zlk.com
LEVI & KORSINSKY, LLP
1101 30th St., NW, Ste. 115
Washington, DC 20007
Telephone: (202) 524-4292
Facsimile: (202) 333-2121

Rosemary M. Rivas, Esq. (to be admitted *pro hac vice*)
Email: rrivas@zlk.com
Rosanne L. Mah, Esq. (to be admitted *pro hac vice*)
Email: rmah@zlk.com
LEVI & KORSINSKY, LLP
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 373-1674
Facsimile: (415) 484-1294

Courtney E. Maccarone, Esq. (to be admitted *pro hac vice*)
Email: cmaccarone@zlk.com
LEVI & KORSINSKY, LLP
55 Broadway, 10th Floor
New York, NY 10006

Telephone: (212) 363-7500
Facsimile: (212) 363-7171

Counsel for Plaintiff CHRIS CERVANTES